

## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

### Listing of Claims:

- 1           1.       (Currently amended) A gateway device disposed between a data  
2 center and a network for thwarting denial of service attacks on the data center, the  
3 gateway device ~~comprises~~ comprising:  
4           a computing device ~~comprising~~ that performs:  
5           a monitoring process that monitors network traffic through the gateway  
6 device;  
7           a communication process that communicates statistics collected in the  
8 gateway from the monitoring process with a control center and that receives  
9 queries or instructions from the control center; and  
10          a filtering process to insert filters on network devices to filter out packets  
11 that the gateway deems to be part of an attack.
  
- 1           2.       (Original) The gateway of claim 1 wherein the communication  
2 process couples to a dedicated link to communicate with the control center over a  
3 hardened network.
  
- 1           3.       (Original) The gateway of claim 1 wherein the monitoring process  
2 in the gateway samples network packet flow in the network.
  
- 1           4.       (Original) The gateway of claim 1 wherein the gateway is  
2 adaptable to be physically deployed in line in the network.

1           5.       (Original) The gateway of claim 1 wherein, the gateway is  
2 adaptable to dynamically install the filters on nearby routers.

1           6.       (Original) The gateway of claim 1 wherein the monitoring process  
2 detects IP traffic and determines levels of unusual amounts of IP fragmentation or  
3 fragmented IP packets with bad or overlapping fragment offsets.

1           7.       (Original) The gateway of claim 1 wherein the monitoring process  
2 detects Internet Protocol (IP) traffic and determines levels of IP packets that have  
3 bad source addresses or Internet Control Message Protocol (ICMP) packets with  
4 broadcast destination addresses.

1           8.       (Currently amended) The gateway of claim 1 wherein the  
2 monitoring process detects Internet Protocol (IP) traffic and determines levels of  
3 Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets  
4 to unused ports.

1           9.       (Currently amended) The gateway of claim 1 wherein the  
2 monitoring process detects IP traffic and determines levels of TCP segments  
3 advertising unusually small window sizes, which may indicate a load on the data  
4 center, or TCP ACK packets not belonging to a known connection.

1           10.      (Currently amended) The gateway of claim 1 wherein the  
2 monitoring process detects sustained rate higher than plausible for a human user  
3 over a persistent HTTP connection.

1           11.      (Currently amended) The gateway of claim 1 wherein the  
2 monitoring process maintains statistical summary information of traffic over  
3 different periods of time and at different levels of detail.

4

5           12.     (Currently amended) The gateway of claim 11 wherein the  
6     monitoring process maintains statistics on parameters including source and  
7     destination host or network addresses, protocols, types of packets, number of  
8     open connections or of packets sent in either direction.

1           13.     (Currently amended) The gateway of claim 12 wherein the  
2     monitoring process has configurable thresholds and issues a warning when one of  
3     the measured parameters exceeds the corresponding threshold.

1           14.     (Currently amended) The gateway of claim 13 wherein the  
2     monitoring process logs packets.

1           15.     (Currently amended) The gateway of claim 14 wherein the  
2     monitoring process logs specific packets identified as part of an attack to enable  
3     an administrator to identify important properties of the attack.

1           16.     (Currently amended) A method of protecting a victim site during a  
2     denial of service attack, ~~comprises~~ comprising:  
3                 disposing a gateway device between the victim site and a network;  
4                 monitoring network traffic through the gateway device and measuring  
5     heuristics of the network traffic to provide statistics network traffic;  
6                 communicating the statistics collected in the gateway device to a control  
7     center; and  
8                 filtering out packets that the gateway or control center deems to be part of  
9     an attack.

1           17.     (Currently amended) The method of claim 16 wherein the  
2     communicating process occurs over a dedicated link to the control center via a  
3     hardened network.

1           18.     (Currently amended) The method of claim 16 wherein the  
2     monitoring process samples network packet flow in the network.

1           19.     (Original) The method of claim 16 wherein the gateway is  
2     physically deployed in line in the network.

1           20.     (Currently amended) The method of claim 16 wherein the filtering  
2     process further comprises:  
3                 dynamically installing filters on nearby routers via an out of band  
4     connection.

1           21.     (Currently amended) The method of claim 16 wherein the  
2     monitoring process further comprises:  
3                 detecting IP traffic and determining levels of unusual amounts of IP  
4     fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

1           22.     (Currently amended) The method of claim 16 wherein the  
2     monitoring process further comprises:  
3                 detecting Internet Protocol (IP) traffic and determining levels of IP  
4     packets that have bad source addresses or Internet Control Message Protocol  
5     (ICMP) packets with broadcast destination addresses.

1           23.     (Currently amended) The method of claim 16 wherein the  
2     monitoring process further comprises:

3 detecting Internet Protocol (IP) traffic and determining levels of Transport  
4 Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

1 24. (Currently amended) The method of claim 16 wherein the  
2 monitoring process further comprises:  
3 detecting IP traffic and determines levels of TCP segments advertising  
4 unusually small window sizes, which may indicate a load on the data center, or  
5 TCP ACK packets not belonging to a known connection.

1 25. (Currently amended) The method of claim 16 wherein the  
2 monitoring process further comprises:  
3 detecting a sustained rate of reload requests that is higher than plausible  
4 for a human user over a persistent HTTP connection.

1 26. (Currently amended) The method of claim 16 wherein the  
2 monitoring process further comprises:  
3 logging statistics on parameters including source and destination host or  
4 network addresses, protocols, types of packets, number of open connections or of  
5 packets sent in either direction.

1 27. (Currently amended) The method of claim 16 wherein the  
2 monitoring process further comprises:  
3 issuing a warning to the control center when one of the measured  
4 parameters exceeds a corresponding configurable threshold.

1 28. (Currently amended) The method of claim 16 wherein the  
2 monitoring process further comprises:  
3 logging specific packets identified as part of an attack to enable an  
4 administrator to identify important properties of the attack.

1           29.     (Currently amended) A computer program product residing on a  
2     ~~non-transitory~~ computer readable storage medium for protecting a victim site  
3     ~~during a denial of service attack, comprises storing instructions that when~~  
4     ~~executed by a computer cause the computer to perform a method for causing a~~  
5     ~~computer device coupled at an entry to the site to~~ protecting a victim site during a  
6     denial of service attack, the method comprising:

7                 ~~monitor~~ monitoring network traffic sent to the victim site and ~~measure~~  
8     measuring heuristics of the network traffic to provide statistics on the network  
9     traffic;

10                ~~communicate~~ communicating the statistics collected in the computer  
11     device to a control center; and

12                ~~filter~~ filtering out packets that the device or control center deems to be  
13     part of an attack.

1           30.     (Currently amended) The computer program product of claim 29,  
2     wherein the monitoring process further comprises sampling network  
3     flow ~~instructions to monitor further comprise instructions to:~~

4                 ~~sample network traffic flow.~~

1           31.     (Currently amended) The computer program product of claim 29,  
2     ~~wherein instructions to filter further comprise instructions to:~~ the filtering process  
3     further comprising:

4                 dynamically ~~install~~ installing filters on nearby routers via an out of band  
5     connection.

1           32.     (Currently amended) The computer program product of claim 29,  
2     ~~wherein instructions to monitor further comprise instructions to~~ the monitoring  
3     process further comprising:

4           ~~detect~~detecting IP traffic; and  
5           ~~determine~~determining levels of unusual amounts of IP fragmentation or  
6 fragmented IP packets with bad or overlapping fragment offsets.

1           33.     (Currently amended) The computer program product of claim 29,  
2 ~~wherein instructions to monitor further comprise instructions to~~ the monitoring  
3 process further comprising :

4           ~~detect~~detecting Internet Protocol (IP) traffic; and  
5           ~~determine~~determining levels of IP packets that have bad source addresses  
6 or Internet Control Message Protocol (ICMP) packets with broadcast destination  
7 addresses.

1           34.     (Currently amended) The computer program product of claim 29,  
2 ~~wherein instructions to monitor further comprise instructions to~~ the monitoring  
3 process further comprising:

4           ~~detect~~detecting Internet Protocol (IP) traffic; and  
5           ~~determine~~determining levels of Transport Control Protocol (TCP) or User  
6 Datagram Protocol UDP packets to unused ports.

1           35.     (Currently amended) The computer program product of claim 29,  
2 ~~wherein instructions to monitor further comprises instructions to~~ the monitoring  
3 process further comprising:

4           ~~detect~~detecting IP traffic; and  
5           ~~determine~~determining levels of TCP segments advertising unusually  
6 small window sizes, which may indicate a load on the data center, or TCP ACK  
7 packets not belonging to a known connection.

1           36.     (Currently amended) The computer program product of claim 29,  
2 ~~wherein instructions to monitor further comprises instructions to~~ the monitoring  
3 process further comprising:  
4           ~~detect~~ detecting a sustained rate of reload requests that is higher than  
5 plausible for a human user over a persistent HTTP connection.

1           37.     (Currently amended) The computer program product of claim 29,  
2 ~~wherein instructions to monitor further comprises instructions to~~ the monitoring  
3 process further comprising:  
4           ~~log~~ logging statistics on parameters including source and destination host  
5 or network addresses, protocols, types of packets, number of open connections or  
6 of packets sent in either direction.

1           38.     (Currently amended) The computer program product of claim 29,  
2 ~~wherein instructions to monitor further comprises instructions to~~ the monitoring  
3 process further comprising:  
4           ~~issue~~ issuing a warning to the control center when one of the measured  
5 parameters exceeds a corresponding configurable threshold.

1           39.     (Currently amended) The computer program of claim 29, ~~further~~  
2 ~~comprising instructions to cause the processor to receive~~ the communicating  
3 process further comprising receiving communications from ~~a~~ the control center to  
4 deliver data pertaining to the types of traffic passing through the gateway.